(併合親 2002-332404
US
924

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１１月１９日

出 願 番 号
Application Number: 特願２００２－３３５４０１

[ST. 10/C]: [ＪＰ２００２－３３５４０１]

出 願 人
Applicant(s): 日本電気株式会社
日本電気通信システム株式会社

２００３年 ９月２５日

特許庁長官
Commissioner,
Japan Patent Office 今 井 康 夫

出証番号 出証特２００３－３０７８９５６

【書類名】　特許願
【整理番号】　49200232
【あて先】　特許庁長官殿
【国際特許分類】　H04L　9/06
H04L　9/14
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　地引　昌弘
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　鈴木　一哉
【発明者】
【住所又は居所】　東京都港区三田一丁目４番２８号　日本電気通信システム株式会社内
【氏名】　馬越　英之
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【特許出願人】
【識別番号】　000232254
【氏名又は名称】　日本電気通信システム株式会社
【代理人】
【識別番号】　100093595
【弁理士】
【氏名又は名称】　松本　正夫
【手数料の表示】
【予納台帳番号】　057794
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9303563

【包括委任状番号】　0100121

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ストリームメディアデータのスクランブル放送システム

【特許請求の範囲】

【請求項１】　配信側がストリームメディアデータを暗号鍵によって符号化して通信回線を介して配信し、受信側が配信されたストリームメディアデータを暗号鍵によって復号化するストリームメディアデータのスクランブル放送システムにおいて、

前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置を備え、

前記配信側は、所定の時間的間隔で、前記鍵ビットパターン生成装置から生成される異なる前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行い、

前記受信側は、前記配信側と同じ前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行うことを特徴とするストリームメディアデータのスクランブル放送システム。

【請求項２】　ストリームメディアデータの一定のデータ量毎に、前記鍵ビットパターンを変更することにより、前記配信側と前記受信側が、前記一定のデータ量に基づいて符号化と復号化に使用する前記鍵ビットパターンを変更することを特徴とする請求項１に記載のストリームメディアデータのスクランブル放送システム。

【請求項３】　入力されたストリームメディアデータに対して、前記鍵ビットパターンを用いて排他的論理和をとることにより、前記符号化と復号化を行うことを特徴とする請求項１又は請求項２に記載のストリームメディアデータのスクランブル放送システム。

【請求項４】　前記ストリームメディアデータの種類に応じて、前記鍵ビットパターンのビット数を増減することを特徴とする請求項１から請求項３の何れか１項に記載のストリームメディアデータのスクランブル放送システム。

【請求項５】　前記鍵ビットパターン生成装置によって生成された前記鍵ビットパターンと、当該鍵ビットパターンを反転させたビットパターンの２つのビ

ットパターンを用いて、前記符号化と復号化を行うことを特徴とする請求項１から請求項４の何れか１項に記載のストリームメディアデータのスクランブル放送システム。

【請求項６】　前記ストリームメディアデータを符号化する際に、前記鍵ビットパターンを一意に識別する情報を、ストリームメディアデータに埋め込むと共に、前記ストリームメディアデータの復号化の際に、前記埋め込まれた前記鍵ビットパターンの情報によって復号化に用いる前記鍵ビットパターンを前記鍵ビットパターン生成装置から取得することを特徴とする請求項１から請求項５の何れか１項に記載のストリームメディアデータのスクランブル放送システム。

【請求項７】　配信側がストリームメディアデータを暗号鍵によって符号化して通信回線を介して配信し、受信側が配信されたストリームメディアデータを暗号鍵によって復号化するストリームメディアデータのスクランブル放送システムにおいて前記ストリームメディアデータの符号化と復号化を実行するスクランブル処理プログラムであって、

前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置を備え、

前記配信側で、所定の時間的間隔で、前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置から生成される異なる前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行う機能を実行し、

前記受信側で、前記配信側と同じ前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行う機能を実行することを特徴とするスクランブル処理プログラム。

【請求項８】　ストリームメディアデータの一定のデータ量毎に、前記鍵ビットパターンを変更することにより、前記配信側と前記受信側が、前記一定のデータ量に基づいて符号化と復号化に使用する前記鍵ビットパターンを変更する機能を有することを特徴とする請求項７に記載のスクランブル処理プログラム。

【請求項９】　入力されたストリームメディアデータに対して、前記鍵ビットパターンを用いて排他的論理和をとることにより、前記符号化と復号化を行う

機能を有することを特徴とする請求項７又は請求項８に記載のスクランブル処理プログラム。

【請求項１０】　前記ストリームメディアデータの種類に応じて、前記鍵ビットパターンのビット数を増減する機能を有することを特徴とする請求項７から請求項９の何れか１項に記載のスクランブル処理プログラム。

【請求項１１】　前記鍵ビットパターン生成装置によって生成された前記鍵ビットパターンと、当該鍵ビットパターンを反転させたビットパターンの２つのビットパターンを用いて、前記符号化と復号化を行うことを特徴とする請求項７から請求項１０の何れか１項に記載のスクランブル処理プログラム。

【請求項１２】　前記ストリームメディアデータを符号化する際に、前記鍵ビットパターンを一意に識別する情報を、ストリームメディアデータに埋め込む機能を有し、前記ストリームメディアデータの復号化の際に、前記埋め込まれた前記鍵ビットパターンの情報によって復号化に用いる前記鍵ビットパターンを前記鍵ビットパターン生成装置から取得する機能を有することを特徴とする請求項７から請求項１１の何れか１項に記載のスクランブル処理プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ストリームメディアデータのスクランブル放送システムに関し、特に専用ハードウェアなどを特に必要とせず簡単に符号化と復号化を行うことを可能とするストリームメディアデータのスクランブル放送システムに関する。

【０００２】

【従来の技術】

インターネットを利用したストリームメディアデータの配信放送、衛星放送、ケーブルテレビ放送などの、ストリームメディアデータの放送については、ビジネス上の理由から、コンテンツの保護を行なうスクランブル放送が要求されている。従来、このストリームメディアデータのスクランブルとしては、主にDESやAES、RSAなどの暗号化アルゴリズムが用いられてきている。

【０００３】

これらのアルゴリズムは、強力な暗号化が可能である一方、ソフトウェアで符号化／復号化を行なうには多くの処理が必要であり、特に放送データのようなリアルタイムの符号化／復号化を行なう場合には、専用のハードウェアが必要である。放送サービス用のスクランブル装置は、各家庭に広く普及させる必要があるものの、このようなコスト面における問題は普及の障壁となっている。

【０００４】

ストリームメディアデータのスクランブル放送方式に関する従来技術としては、例えば、特開平８－２８８９３９号公報に開示されている技術等が提案されている。この特開平８－２８８９３９号公報においては、回線終端装置の暗号鍵発生部によって生成される暗号鍵によって放送セルを暗号化すると共に、加入者端末が予め付与された暗号鍵を用いて放送セルを復号化する方法が開示されている。

【０００５】

【発明が解決しようとする課題】

上述したように、従来のストリームメディアデータのスクランブル放送方式では、特殊な暗号化アルゴリズムを用いるためストリームメディアデータのスクランブルのために専用のハードウェアを備える必要があるため、ストリームメディアデータの配信及び受信を行うためにコストがかかり、普及を妨げる要因となっていた。

【０００６】

例えば、上述した特開平８－２８８９３９号公報の技術でも、暗号鍵によって放送セルを暗号化するための、及び暗号化された放送セルを復号するための専用のハードウェア装置が必要となる。

【０００７】

本発明の目的は、ストリームメディアデータに対して高速な符号化と復号化を施し、スクランブル放送を符号化及び復号化のための専用ハードウェアなどを特に必要とせず簡単に行なうことを可能にするストリームメディアデータのスクランブル放送方式を提供することにある。

【０００８】

本発明の他の目的は、ソフトウェアによる処理でも高速な符号化及び復号化を行なうことができるストリームメディアデータのスクランブル放送方式を提供することにある。

【０００９】

本発明のさらに他の目的は、ストリームメディアデータのスクランブルにおける鍵の強度を実用的なレベルまで上げることができるストリームメディアデータのスクランブル放送方式を提供することにある。

【００１０】

【課題を解決するための手段】

上記目的を達成する本発明は、配信側がストリームメディアデータを暗号鍵によって符号化して通信回線を介して配信し、受信側が配信されたストリームメディアデータを暗号鍵によって復号化するストリームメディアデータのスクランブル放送システムにおいて、前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置を備え、前記配信側は、所定の時間的間隔で、前記鍵ビットパターン生成装置から生成される異なる前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行い、前記受信側は、前記配信側と同じ前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行うことを特徴とする。

【００１１】

請求項２の本発明のスクランブル放送システムは、ストリームメディアデータの一定のデータ量毎に、前記鍵ビットパターンを変更することにより、前記配信側と前記受信側が、前記一定のデータ量に基づいて符号化と復号化に使用する前記鍵ビットパターンを変更することを特徴とする。

【００１２】

請求項３の本発明のスクランブル放送システムは、入力されたストリームメディアデータに対して、前記鍵ビットパターンを用いて排他的論理和をとることにより、前記符号化と復号化を行うことを特徴とする。

【００１３】

請求項４の本発明のスクランブル放送システムは、前記ストリームメディアデ

ータの種類に応じて、前記鍵ビットパターンのビット数を増減することを特徴とする。

【００１４】

請求項５の本発明のスクランブル放送システムは、前記鍵ビットパターン生成装置によって生成された前記鍵ビットパターンと、当該鍵ビットパターンを反転させたビットパターンの２つのビットパターンを用いて、前記符号化と復号化を行うことを特徴とする。

【００１５】

請求項６の本発明のスクランブル放送システムは、前記ストリームメディアデータを符号化する際に、前記鍵ビットパターンを一意に識別する情報を、ストリームメディアデータに埋め込むと共に、前記ストリームメディアデータの復号化の際に、前記埋め込まれた前記鍵ビットパターンの情報によって復号化に用いる前記鍵ビットパターンを前記鍵ビットパターン生成装置から取得することを特徴とする。

【００１６】

請求項７の本発明は、配信側がストリームメディアデータを暗号鍵によって符号化して通信回線を介して配信し、受信側が配信されたストリームメディアデータを暗号鍵によって復号化するストリームメディアデータのスクランブル放送システムにおいて前記ストリームメディアデータの符号化と復号化を実行するスクランブル処理プログラムであって、前記配信側で、所定の時間的間隔で、前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置から生成される異なる前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行う機能を実行し、前記受信側で、前記配信側と同じ前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行う機能を実行することを特徴とする。

【００１７】

請求項８の本発明のスクランブル処理プログラムは、ストリームメディアデータの一定のデータ量毎に、前記鍵ビットパターンを変更することにより、前記配信側と前記受信側が、前記一定のデータ量に基づいて符号化と復号化に使用する前

記鍵ビットパターンを変更する機能を有することを特徴とする。

【００１８】

請求項９の本発明のスクランブル処理プログラムは、入力されたストリームメディアデータに対して、前記鍵ビットパターンを用いて排他的論理和をとることにより、前記符号化と復号化を行う機能を有することを特徴とする。

【００１９】

請求項１０の本発明のスクランブル処理プログラムは、前記ストリームメディアデータの種類に応じて、前記鍵ビットパターンのビット数を増減する機能を有することを特徴とする。

【００２０】

請求項１１の本発明のスクランブル処理プログラムは、前記鍵ビットパターン生成装置によって生成された前記鍵ビットパターンと、当該鍵ビットパターンを反転させたビットパターンの２つのビットパターンを用いて、前記符号化と復号化を行うことを特徴とする。

【００２１】

請求項１２の本発明のスクランブル処理プログラムは、前記ストリームメディアデータを符号化する際に、前記鍵ビットパターンを一意に識別する情報を、ストリームメディアデータに埋め込む機能を有し、前記ストリームメディアデータの復号化の際に、前記埋め込まれた前記鍵ビットパターンの情報によって復号化に用いる前記鍵ビットパターンを前記鍵ビットパターン生成装置から取得する機能を有することを特徴とする。

【００２２】

【発明の実施の形態】

以下、本発明の好ましい実施の形態について図面を参照して詳細に説明する。

【００２３】

図１は、本発明によるストリームメディアデータのスクランブル放送方式を適用した実施の形態のシステム構成を示すブロック図である。

【００２４】

この実施の形態によるシステムは、ストリームメディアデータの符号化（スク

ランブル）"を行なうスクランブル装置１０と、符号化されたストリームメディアデータの復号化（スクランブルの解除）を行なうスクランブル解除装置２０、及び符号化／復号化処理において排他的論理和を取るための鍵ビットパターンを生成する鍵ビットパターン生成装置３０を含む。

【００２５】

スクランブル装置１０は、図２に示す一例のように、インターネット等の通信回線上でコンテンツであるストリームメディアデータの配信サービスを行うサービス業者（サービスプロバイダ等）のサーバ１００等にその機能として又はオプションとして備えられる装置であり、入力された生ストリームメディアデータに対し、鍵ビットパターン生成装置３０から配布されて鍵ビットパターン管理部１１が管理する所定の鍵ビットパターンを用いて、ストリーム符号化部１２において排他的論理和による符号化処理を行う。

【００２６】

また、符号化されたストリームメディアデータには、符号化に利用した鍵ビットパターンを一意に識別する識別情報が埋め込まれる。この識別情報により、スクランブル解除装置２０においてストリームメディアデータの復号化を行う際に、必要な鍵ビットパターンを鍵ビットパターン生成装置３０に要求することができる。

【００２７】

なお、スクランブル装置１０は、上記のようにインターネット等の通信回線上でコンテンツであるストリームメディアデータの配信サービスを行うサービス業者に限らず、衛星放送やケーブルテレビ放送を行うサービス業者のストリームメディアデータの配信装置にも、その機能として又はオプションとして備えられる。

【００２８】

符号化されたストリームメディアデータは、ストリーム符号化部１２から出力され、インターネット等のネットワーク上をパケット通信等により配信されてスクランブル解除装置２０へ入力される。

【００２９】

このスクランブル解除装置２０は、図２に示す一例のようにコンテンツである

ストリームメディアデータの配信を受ける（放送を受信する）ユーザのクライアント端末（受信装置）２００に、その機能として又はオプション（例えば、クライアント端末とモデムとの間に介在）として備えられる装置であり、入力された符号化ストリームメディアデータに対し、鍵ビットパターン生成装置３０から配布されて鍵ビットパターン管理部２１が管理する所定の鍵ビットパターンを用いて、ストリーム復号化部２２において排他的論理和による復号化処理を行う。復号化されたストリームメディアデータは、ストリーム復号化部２２から出力され、ユーザのクライアント端末２００へ提供され、画像表示装置上に表示される。

【００３０】

なお、ケーブルテレビ放送を受信するユーザであれば、上記スクランブル解除装置２０は、例えばケーブルテレビのセットトップボックスの機能又はオプションとして備えられる。

【００３１】

鍵ビットパターン生成装置３０は、インターネット等の通信回線を介して上記放送サービス業者のサーバ１００等の装置及びユーザのクライアント端末２００等の装置と接続され、それぞれに対してストリームメディアデータの排他的論理和による符号化と復号化に利用する所定の鍵ビットパターンを生成して配布する。

【００３２】

この鍵ビットパターン生成装置３０は、図２に示す一例のように、サービス業者及びユーザに対して所定の鍵ビットパターンの配布を行う独立した鍵ビットパターン配布サービス業者のサーバ３００に、その機能として又はオプションとして備えられている。

【００３３】

鍵ビットパターン管理部１１及び鍵ビットパターン管理部２１は、定期的あるいは所定のデータ量ごとに鍵ビットパターン生成装置３０に対して鍵ビットパターンの配布を要求する。

【００３４】

また、鍵ビットパターン配布サービス業者のサーバ３００では、ストリームメデ

ィアデータを受信するユーザ毎に、鍵ビットパターンの配布量（配布数）を計数して管理することにより、その計数値に応じてユーザからコンテンツの課金（視聴料）を徴収し、放送サービス業者に対して支払うといったサービスを行うこともできる。

【００３５】

このようにストリームメディアデータの復号化に必要な鍵ビットパターンの配布量に応じて課金を徴収することにより、確実に配信を受けたストリームメディアデータ量に応じた適切な課金を行うことができると共に、放送サービス業者にとっても課金徴収に伴う負担を軽減することができる。

【００３６】

次いで、上記のように構成される本システムの動作について図１～図６を参照して詳細に説明する。

【００３７】

まず、生ストリームメディアデータに対して符号化処理（スクランブル処理）を行う動作について説明する。

【００３８】

図１のスクランブル装置１０に対して入力された生ストリームメディアデータは、鍵ビットパターン管理部１１が管理する所定の鍵ビットパターンを用いて、ストリーム符号化部１２において符号化されるが、図３及び図４と、図７のフローチャートを参照してその詳細なアルゴリズムを説明する。

【００３９】

図３、図４に示す生ストリームメディアデータ４０は、スクランブル装置１０に入力された符号化される前のストリームメディアデータである。鍵ビットパターン５０は、鍵ビットパターン生成装置３０が生成し、鍵ビットパターン管理部１１を経由して渡される生ストリームメディアデータ４０との排他的論理和をとるための鍵ビットパターンである。鍵ビットパターン５０のビット数は任意であるが、図３から図６の符号化処理及び復号化処理では４ビットである場合を例として説明する。

【００４０】

この鍵ビットパターンとしては、実際の運用においては、例えば３２ビット、１２８ビット、５１２ビット等のビット数が利用される。符号化したストリームメディアデータの機密性は、鍵ビットパターンの鍵として強度に比例して大きくなるので、機密性を大きくしたい場合には鍵ビットパターンのビット数を増やし容易に解除できないようにする。ただし、鍵ビットパターンのビット数を必要以上に大きくしても機密性の大きさは余り変わらず、処理だけに時間がかかってしまうことになる。

【００４１】

ストリームメディアデータの種類（映画やニュース等）に応じて、すなわち機密性に応じて、鍵ビットパターンのビット数を変更するようにすることもできる。

【００４２】

スクランブル装置１０は、生ストリームメディアデータ４０の入力を受け付けると（図７、ステップ１０１）、この生ストリームメディアデータ４０のスクランブル処理を行う鍵となる鍵ビットパターン５０が鍵ビットパターン管理部１１に存在するかどうかを確認する（ステップ１０２）。すなわち、現在使用している鍵ビットパターン５０が鍵ビットパターン管理部１１に存在するかを確認する。鍵ビットパターン管理部１１では、現在符号化に使用している鍵ビットパターンを、鍵ビットパターンが変更されるまで保持している。

【００４３】

もし、鍵ビットパターン５０が存在しない場合は、鍵ビットパターン生成装置３０に対して要求を出して鍵ビットパターンを受け取る（ステップ１０３）。鍵ビットパターン５０を保持している場合は、以下の手順で符号化処理を実行する（ステップ１０４からステップ１０８）。

【００４４】

まず、生ストリームメディアデータ４０の先頭から４ビット（ビット番号１～ビット番号４の「１００１」）のデータと鍵ビットパターン５０との排他的論理和をとる（ステップ１０５）。

【００４５】

全ての生ストリームメディアデータ４０についてスクランブルを行ったかを判定しながら（ステップ１０６）、生成されたビット列「０１００」を、スクランブルストリームデータ６１として保存する（ステップ１０７）。

【００４６】

続いて、生ストリームメディアデータ４０における次の４ビット（ビット番号５～ビット番号８の「１０１０」）のデータと鍵ビットパターン５０との排他的論理和をとる。生成されたビット列「０１１１」は、保存されているスクランブルストリームデータ６１の続きに連結される。この手順を繰り返し、生ストリームメディアデータ４０における全てのビットに対して鍵ビットパターン５０による排他的論理和をとる処理を終了した後、最終的に生成され保存されているスクランブルストリームデータ６１を出力する（ステップ１０８）。スクランブルストリームデータ６１は、パケット通信等により通信回線を介してユーザのクライアント端末２００に送られ、スクランブル解除装置２０に入力される。

【００４７】

なお、上記符号化処理に際して、ストリームメディアデータの所定のデータ量単位ごとに、例えばＭＰＥＧデータであれば、所定パケット数毎に、又は所定の時間間隔ごとに、鍵ビットパターン生成装置３０に要求することにより、使用する鍵ビットパターンを変更する。

【００４８】

また、鍵ビットパターンを変更するたびに、符号化処理に用いた鍵ビットパターンを一意に識別するための識別情報を埋め込む。パケットであれば、そのヘッダ部分に埋め込む。

【００４９】

次に、スクランブル解除装置２０において、スクランブルされたストリームメディアデータからスクランブルを外し、生ストリームメディアデータを取り出す動作について図５及び図６、図８のフローチャートを参照して説明する。

【００５０】

図１のスクランブル解除装置２０に対して入力されるスクランブルされたストリームメディアデータ（スクランブル装置１０の出力であるスクランブルストリ

ームデータ６１）は、鍵ビットパターン管理部２１が管理する鍵ビットパターンを用いて、ストリーム復号化部２２において復号化されるが、図５、図６を参照してその詳細なアルゴリズムを説明する。

【００５１】

図５、図６のスクランブルストリームデータ６１は、鍵ビットパターン管理部２１に入力された符号化処理された（スクランブルされた）ストリームメディアデータである。

【００５２】

スクランブルストリームデータ６１を復号化する（スクランブルを解除する）鍵ビットパターン８０は、鍵ビットパターン生成装置３０が生成し、鍵ビットパターン管理部２１を経由して渡されるスクランブルストリームデータ６１との排他的論理和をとるための鍵ビットパターンである。この鍵ビットパターン８０は、スクランブル装置１０で生ストリームメディアデータ４０に対して排他的論理和をとり、スクランブルストリームデータ６１を生成するに利用した鍵ビットパターン５０と同じビットパターンを有する。

【００５３】

スクランブル解除装置２０は、スクランブルストリームデータ６１の入力を受け付けると（図８、ステップ２０１）、このスクランブルストリームデータ６１のスクランブルを解除する鍵となる鍵ビットパターンが鍵ビットパターン管理部２１に存在するかどうかを確認する（ステップ２０２）。もし、鍵ビットパターンが存在しない場合は、スクランブルストリームデータ６１に埋め込まれている鍵ビットパターンの識別情報に基づいて鍵ビットパターン生成装置３０に当該鍵ビットパターンの配布を要求して受け取る（ステップ２０３）。すなわち、現在使用している鍵ビットパターン８０が鍵ビットパターン管理部２１に存在するかを確認する。ビットパターン管理部２１では、現在復号化に使用している鍵ビットパターンを、鍵ビットパターンが変更されるまで保持している。

【００５４】

鍵ビットパターン８０を保持している場合又は鍵ビットパターン８０を取得した場合、以下の手順で復号化処理を行う（スクランブルを解除する）（ステップ

２０４からステップ２０８）。

【００５５】

まず、スクランブルストリームデータ６１の先頭から４ビット（ビット番号１～ビット番号４の「０１００」）のデータと鍵ビットパターン８０との排他的論理和をとる（ステップ２０５）。

【００５６】

全てのスクランブルストリームデータ６１についてのスクランブル解除が終了するまで（ステップ２０６）、生成されたビット列「１００１」は、生ストリームメディアデータ９１として保存する（ステップ２０７）。

【００５７】

続いて、スクランブルストリームデータ６１における次の４ビット（ビット番号５～ビット番号８の「０１１１」）のデータと鍵ビットパターン８０との排他的論理和をとる。生成されたビット列「１０１０」は、保存されている生ストリームメディアデータ９１の続きに連結して保存される。この手順を繰り返し、スクランブルストリームデータ６１における全てのビットに対して鍵ビットパターン８０との排他的論理和をとる処理を終了した後、最終的に生成され保存されている生ストリームメディアデータ９１を生ストリームメディアデータとして出力する（ステップ２０８）。

【００５８】

スクランブル装置１０とスクランブル解除装置２０との間では、ストリームメディアデータの所定単位データ量毎に鍵ビットパターンを変更することを予め取り決めておくことにより、スクランブル装置１０では所定単位データ量毎に、或いは所定の時間間隔毎に、新たな鍵ビットパターンを鍵ビットパターン生成装置３０から取得して符号化処理を行う共に、スクランブル解除装置２０では所定単位データ量毎に、スクランブルストリームデータに埋め込まれている識別情報によって新たな鍵ビットパターンを鍵ビットパターン生成装置３０から取得して復号化処理を行うようにすれば、符号化と復号化の同期を取ることができる。

【００５９】

次に、本発明の他の実施の形態について図面を参照して詳細に説明する。

【００６０】

図３から図６の例では、あるストリームメディアデータのある一定量について、１種類の鍵ビットパターンを用いて符号化処理と復号化処理を行なっている。

【００６１】

しかし、複数の鍵ビットパターン生成装置２０から取得した複数の鍵ビットパターンを同時に用いる、あるいは異なるタイミングで取得した複数の鍵ビットパターンを同時に用いる、あるいは１種類の鍵ビットパターンを反転させて生成した複数の鍵ビットパターンを同時に用いる、あるいはこれらの方法を組み合わせることで、複数の鍵ビットパターンを用いた符号化処理と復号化処理を行なうことも可能である。

【００６２】

上記のような方法を用いることにより、１種類の鍵ビットパターンを用いる場合に比べてスクランブルの強度（機密性）を上げることができる。これにより、より多くの種類のストリームメディアデータに対して本発明を適用することができるようになる。

【００６３】

図９は、２つの鍵ビットパターンを用いてスクランブル化を行う例を示している。この例では、鍵ビットパターン５５は、鍵ビットパターン５０を反転させることにより生成している。この鍵ビットパターンの反転は、スクランブル装置１０及びスクランブル解除装置２０において行われる。これにより、スクランブル装置１０及びスクランブル解除装置２０では、１つの鍵ビットパターンを共有するだけで、事実上、２つの鍵ビットパターンによる符号化処理及び復号化処理を施すことができる。

【００６４】

図９では、入力された生ストリームメディアデータ４０に対して、鍵ビットパターン５０及び５５により排他的論理和をとって符号化することにより、スクランブルストリームデータ３０３を生成している。生ストリームメディアデータ３００のビット番号９以降のデータに対しても、鍵ビットパターン５０及び５５をその順で適用して排他的論理和をとり、最終的にネットワーク上を配信可能なス

クランブルメディアデータ３０３を生成する。

【００６５】

図１０は、２つの鍵ビットパターン９０と９５を用いてスクランブルを解除する例を示している。鍵ビットパターン９０及び９５は、それぞれ図９においてスクランブルを施す際に用いた鍵ビットパターン５０、５５と同じ鍵ビットパターンである。スクランブルストリームデータ３０３に対して、鍵ビットパターン９０及び９５により排他的論理和をとって復号化することにより、生ストリームメディアデータ４０１を生成している。スクランブルストリームデータ３０３のビット番号９以降のデータに対しても、鍵ビットパターン９０及び９５をその順で適用して排他的論理和をとり、生ストリームメディアデータ４０１を再生成する。

【００６６】

本発明のストリームメディアデータのスクランブル放送方式は、構成要素である各装置の機能をハードウェア的に実現することは勿論として、上記した各装置の機能を実行してストリームメディアデータのスクランブルとスクランブルの解除を行うスクランブル処理プログラム（アプリケーション）を放送サービス業者のサーバ及びユーザのクライアント端末のコンピュータ処理部（ＣＰＵ）のメモリにロードして実行することで実現することができる。すなわち、スクランブル処理装置及びスクランブル解除装置の機能をソフトウェアによって実現することができる。このスクランブル処理プログラムは、磁気ディスク、半導体メモリその他の記録媒体に格納され、その記録媒体からコンピュータ処理部にロードされ、コンピュータ処理部の動作を制御することにより、上述した各機能を実現する。

【００６７】

以上好ましい実施の形態及び実施例をあげて本発明を説明したが、本発明は必ずしも上記実施の形態及び実施例に限定されるものではなく、その技術的思想の範囲内において様々に変形して実施することができる。

【００６８】

なお、上記実施の形態においては、ストリームデータに埋め込まれた鍵ビットパ

ターンの識別情報に基づいて、スクランブル解除装置が、鍵ビットパターン生成装置に対して鍵ビットパターンの生成を要求する場合を示したが、ストリームデータに鍵ビットパターンの識別情報を埋め込まず、スクランブル解除装置がスクランブル装置に鍵ビットパターンの識別情報を問い合わせるようにすることも可能である。

【００６９】

【発明の効果】

以上説明したように本発明のストリームメディアデータのスクランブル放送方式によれば、以下に述べるような優れた効果が得られる。

【００７０】

ストリームメディアデータに対して高速な符号化と復号化を施し、スクランブル放送を簡潔に行なえるようになる。また、符号化及び復号化のための専用ハードウェアなどを特に必要とせず、携帯端末や家庭内のホームゲートウェイといった小規模な装置でも、符号化及び復号化を用いたストリームメディアデータの放送と受信を容易に行なうことができる。そのため、スクランブル装置及びスクランブル解除装置のコストを従来より引き下げることが可能となり、一般に広く普及させることができる。これにより、パケット通信を用いた放送サービスを本格的に立ち上げることが可能になる。

【００７１】

その理由は、本発明で符号化及び復号化のために利用している鍵ビットパターンによる排他的論理和の処理は、多くのＣＰＵにおいて機械語レベルの命令として実装されているため、ソフトウェアによる処理でも高速に行なえるからである。

【００７２】

なお、スクランブルにおける鍵の強度は、以下の理由により、鍵ビットパターンの有効時間を制限して適宜パターンを変更することにより、実用的なレベルまで上げることができる。

【００７３】

第１に、文字データなどに比べ、ストリームメディアデータでは元の（生の）

データを類推することが困難なため、鍵空間の先頭から鍵を単純に当てはめて解読に成功したかどうかを調べる手法（ＤＥＳの暗号解読に用いられた手法）や、符号化されたデータを多数収集した後にその傾向を調べるといった手法（一般的暗号解読手法）では解読しにくいこと。すなわち、鍵ビットパターンによる排他的論理和処理を利用した符号化及び復号化によって実用的な鍵の強度を持たせることができる。

【００７４】

第２に、ストリームメディアデータ自身が時間と相関した価値を有する場合（例えばニュースの配信など）では、配信から時間を経たデータは情報としての価値が落ちるため、解読に時間をかけることができない。よって、ニュース等のストリームメディアデータの場合には、鍵ビットパターンのビット数が少なくても実用的な鍵の強度を持たせることができる。

【００７５】

第３に、排他的論理和の処理は簡単に行なえるため、鍵（ビットパターン）のサイズを必要十分な強度まで増やしても、符号化及び復号化の処理にはあまり影響を与えない。よって、鍵ビットパターンのビット数を増やすことで十分な鍵の強度を与えることができる。

【図面の簡単な説明】

【図１】　本発明の第１の実施の形態によるストリームメディアデータのスクランブル放送システムの構成を示すブロック図である。

【図２】　本発明の第１の実施の形態によるストリームメディアデータのスクランブル放送システムの全体構成示す図である。

【図３】　本発明の鍵ビットパターンを用いて符号化する際のアルゴリズムを説明する図である。

【図４】　本発明の鍵ビットパターンを用いて符号化する際のアルゴリズムを説明する図である。

【図５】　本発明の鍵ビットパターンを用いて復号化する際のアルゴリズムを説明する図である。

【図６】　本発明の鍵ビットパターンを用いて復号化する際のアルゴリズム

を説明する図である。

【図７】　鍵ビットパターンを用いて符号化するスクランブル装置の動作を説明するフローチャートである。

【図８】　鍵ビットパターンを用いて復号化するスクランブル解除装置の動作を説明するフローチャートである。

【図９】　２つの鍵ビットパターンを用いて符号化を行う際のアルゴリズムを説明する図である。

【図１０】　２つの鍵ビットパターンを用いて復号化を行う際のアルゴリズムを説明する図である。

【符号の説明】

１０　スクランブル装置

１１　鍵ビットパターン管理部

１２　ストリーム符号化部

２０　スクランブル解除装置

２１　鍵ビットパターン管理部

２２　ストリーム復号化部

３０　鍵ビットパターン生成装置

４０　生ストリームメディアデータ

５０　鍵ビットパターン

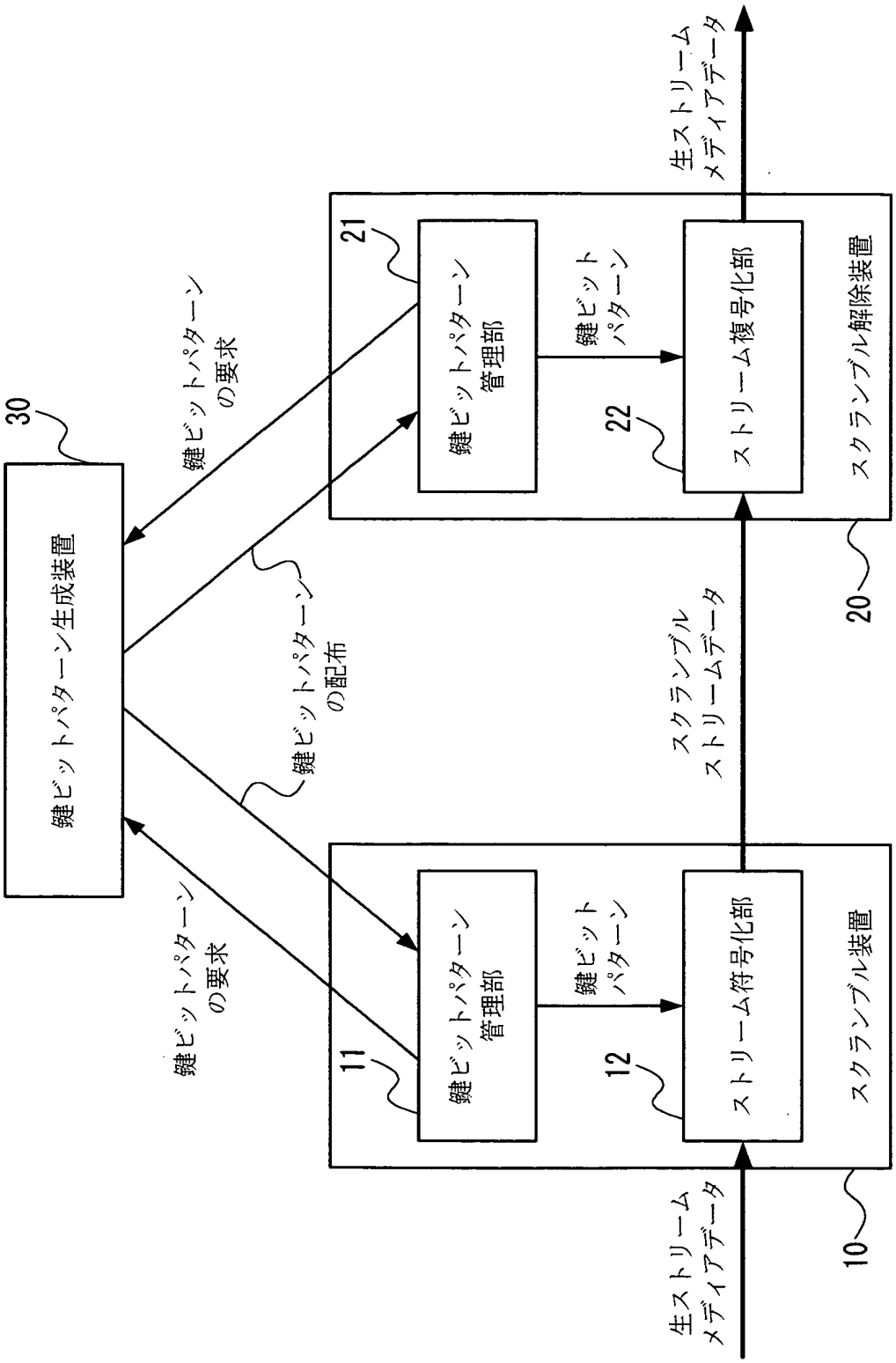
６１　スクランブルストリームデータ

８０　鍵ビットパターン

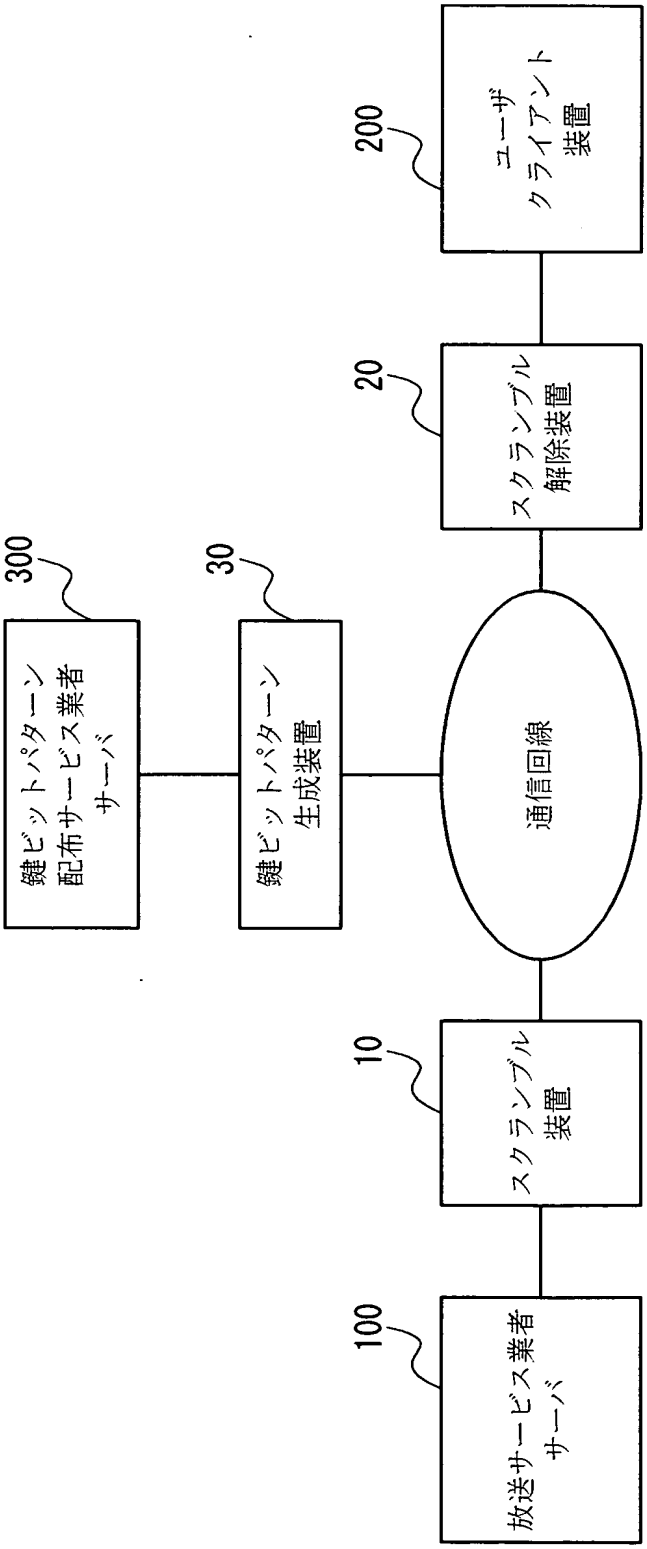
９１　生ストリームメディアデータ

【書類名】　　図面

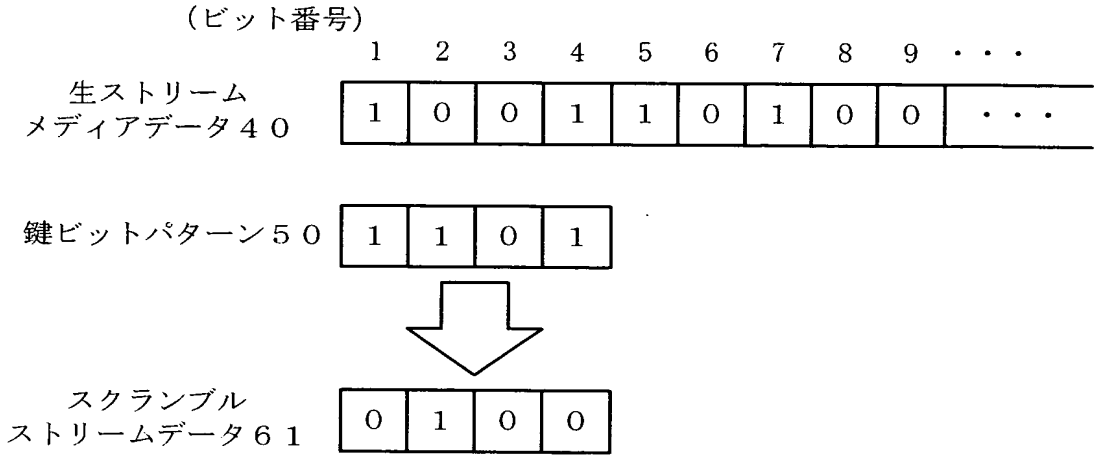
【図１】


鍵ビットパターン生成装置
30
鍵ビットパターン
の要求
鍵ビットパターン
の配布
鍵ビットパターン
の要求
スクランブル
ストリームデータ
生ストリーム
メディアデータ
生ストリーム
メディアデータ
スクランブル装置
10
鍵ビットパターン
管理部
11
鍵ビット
パターン
ストリーム符号化部
12
スクランブル解除装置
20
鍵ビットパターン
管理部
21
鍵ビット
パターン
ストリーム複号化部
22

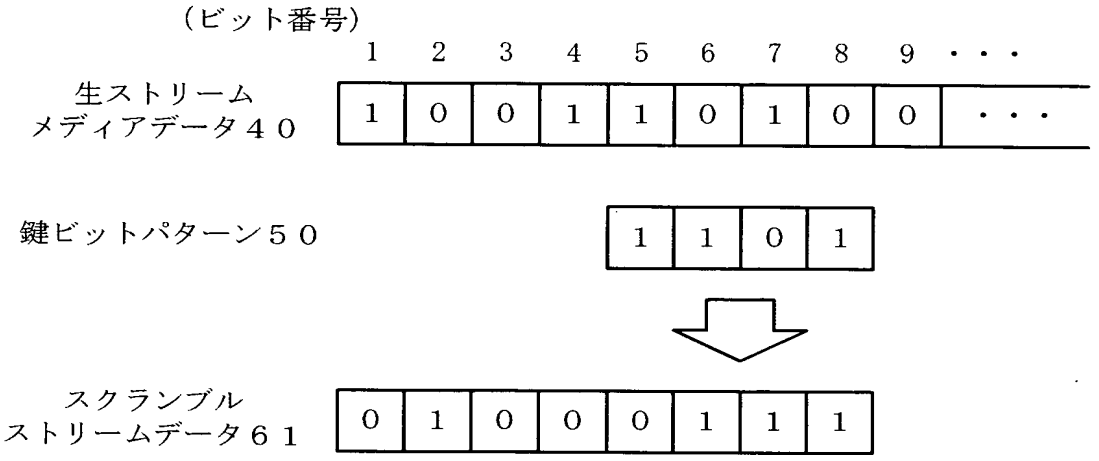
【図２】


ユーザ
クライアント
装置
200
スクランブル
解除装置
20
通信回線
鍵ビットパターン
生成装置
30
鍵ビットパターン
配布サービス業者
サーバ
300
スクランブル
装置
10
放送サービス業者
サーバ
100

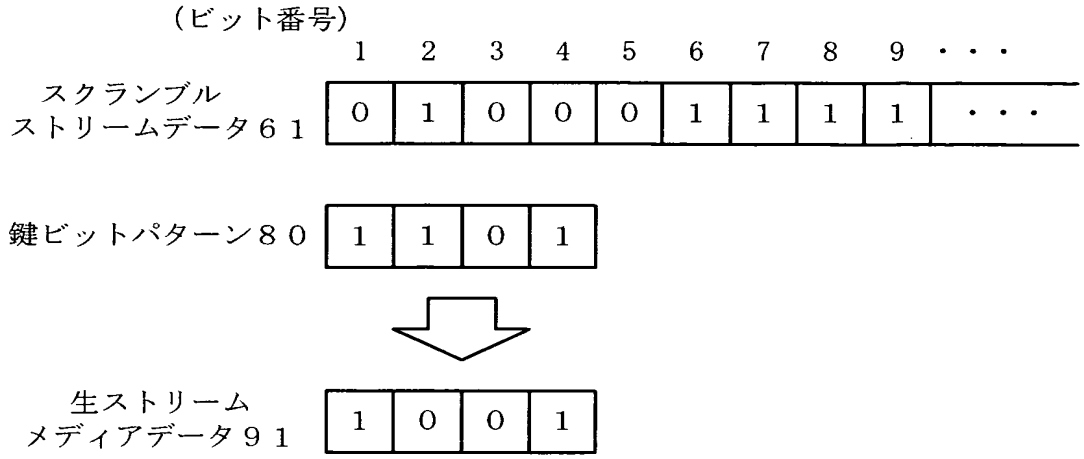
【図３】


（ビット番号）
1 2 3 4 5 6 7 8 9 ・・・
生ストリーム
メディアデータ４０
1 0 0 1 1 0 1 0 0 ・・・
鍵ビットパターン５０
1 1 0 1
スクランブル
ストリームデータ６１
0 1 0 0

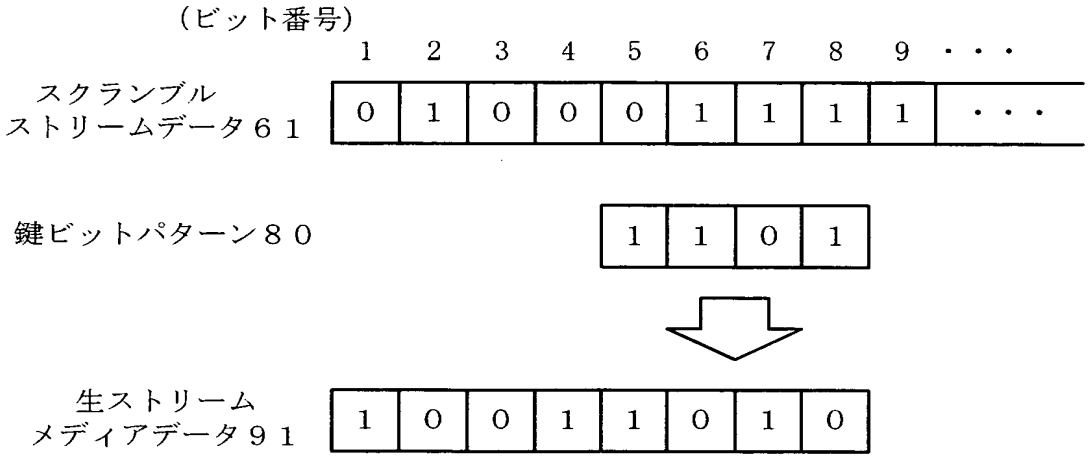
【図４】


（ビット番号）
1 2 3 4 5 6 7 8 9 ・・・
生ストリーム
メディアデータ４０
1 0 0 1 1 0 1 0 0 ・・・
鍵ビットパターン５０
1 1 0 1
スクランブル
ストリームデータ６１
0 1 0 0 0 1 1 1

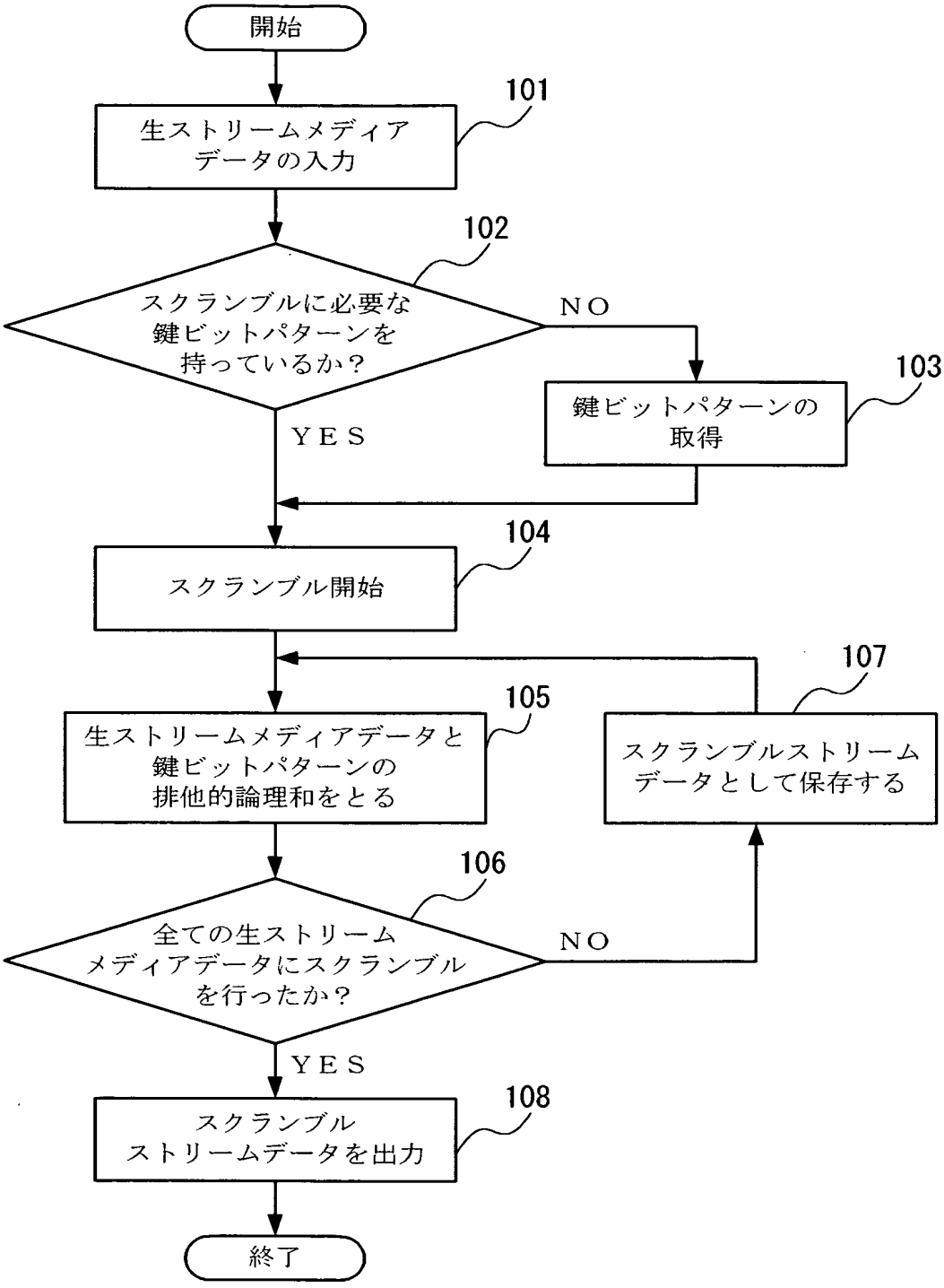
【図５】


（ビット番号）
1 2 3 4 5 6 7 8 9 ・・・
スクランブル
ストリームデータ６１
0 1 0 0 0 1 1 1 1 ・・・
鍵ビットパターン８０
1 1 0 1
生ストリーム
メディアデータ９１
1 0 0 1

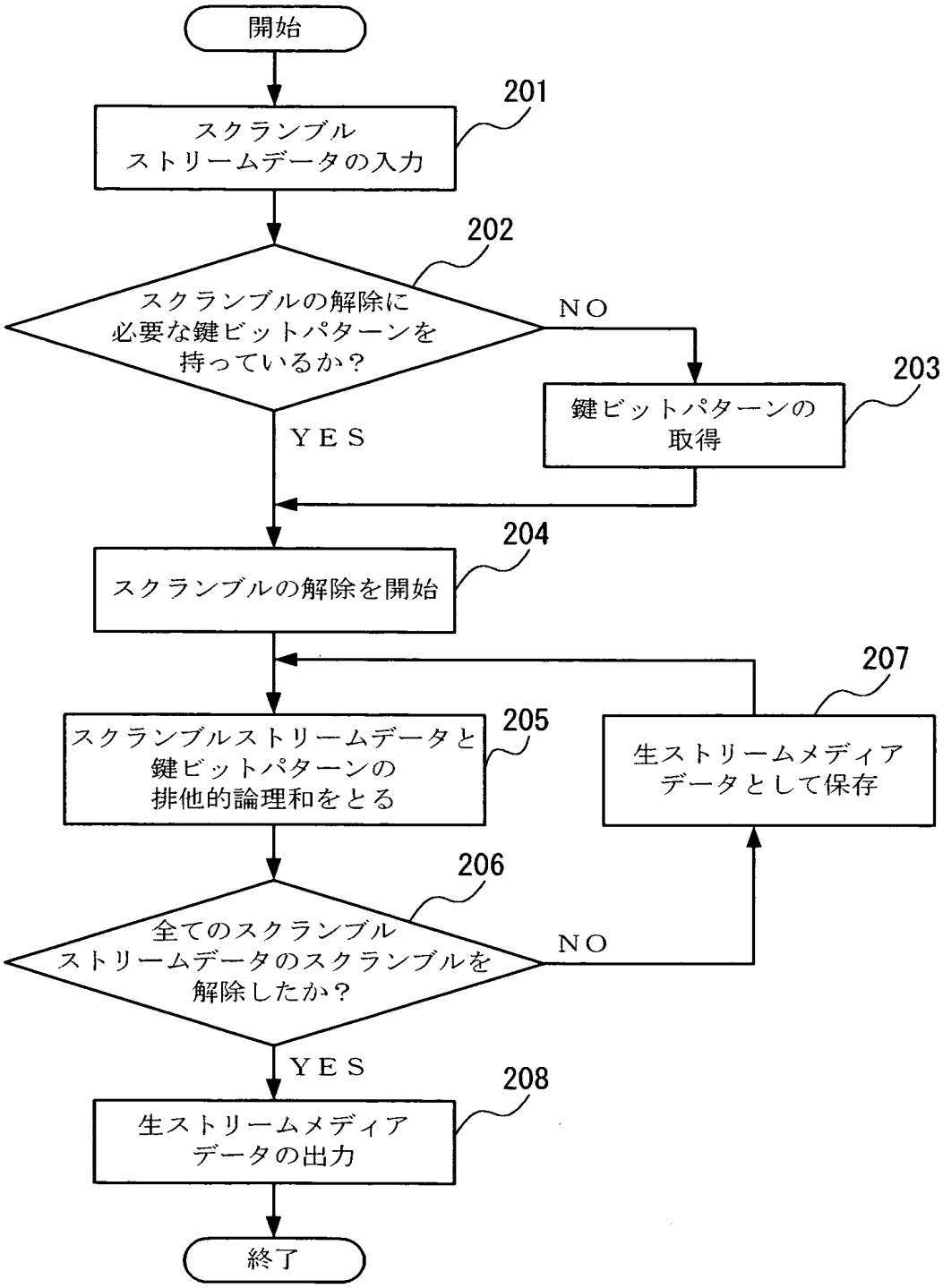
【図６】


（ビット番号）
1 2 3 4 5 6 7 8 9 ・・・
スクランブル
ストリームデータ６１
0 1 0 0 0 1 1 1 1 ・・・
鍵ビットパターン８０
1 1 0 1
生ストリーム
メディアデータ９１
1 0 0 1 1 0 1 0

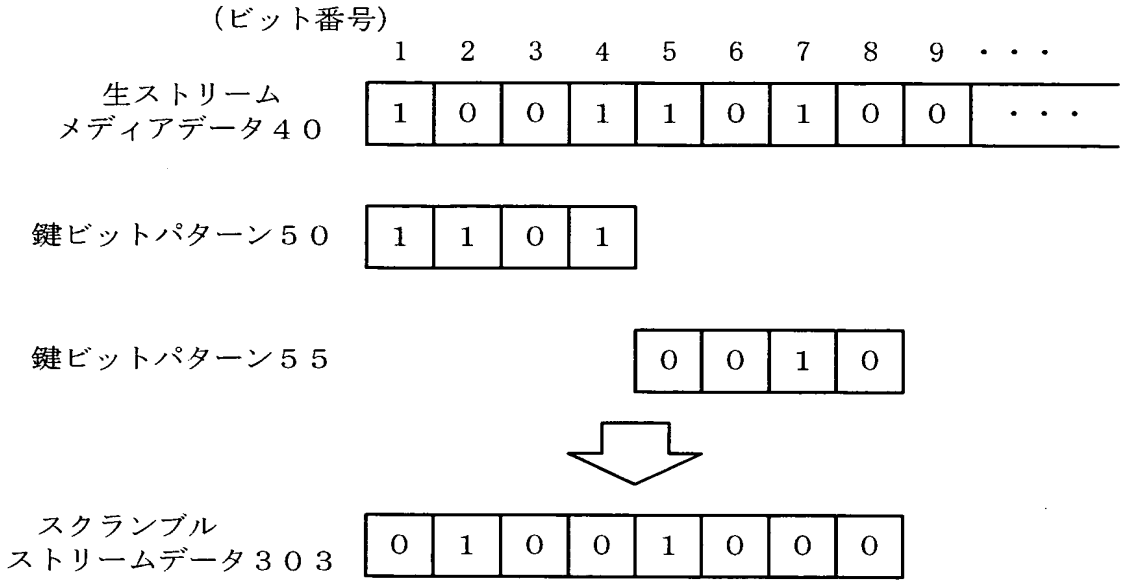
【図７】


開始
101
生ストリームメディア
データの入力
102
スクランブルに必要な
鍵ビットパターンを
持っているか？
NO
103
鍵ビットパターンの
取得
YES
104
スクランブル開始
107
105
生ストリームメディアデータと
鍵ビットパターンの
排他的論理和をとる
スクランブルストリーム
データとして保存する
106
全ての生ストリーム
メディアデータにスクランブル
を行ったか？
NO
YES
108
スクランブル
ストリームデータを出力
終了

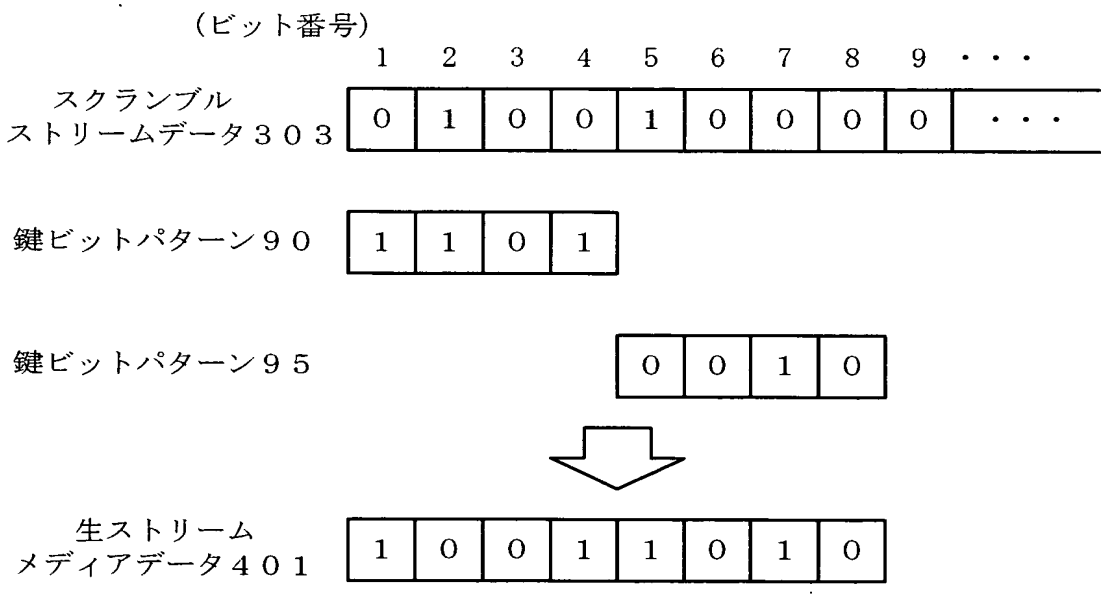
【図８】


開始
201
スクランブル
ストリームデータの入力
202
スクランブルの解除に
必要な鍵ビットパターンを
持っているか？
NO
YES
203
鍵ビットパターンの
取得
204
スクランブルの解除を開始
205
スクランブルストリームデータと
鍵ビットパターンの
排他的論理和をとる
207
生ストリームメディア
データとして保存
206
全てのスクランブル
ストリームデータのスクランブルを
解除したか？
NO
YES
208
生ストリームメディア
データの出力
終了

【図９】


（ビット番号）
1 2 3 4 5 6 7 8 9 ・・・
生ストリーム
メディアデータ４０
1 0 0 1 1 0 1 0 0 ・・・
鍵ビットパターン５０
1 1 0 1
鍵ビットパターン５５
0 0 1 0
スクランブル
ストリームデータ３０３
0 1 0 0 1 0 0 0

【図１０】


（ビット番号）
1 2 3 4 5 6 7 8 9 ・・・
スクランブル
ストリームデータ３０３
0 1 0 0 1 0 0 0 0 ・・・
鍵ビットパターン９０
1 1 0 1
鍵ビットパターン９５
0 0 1 0
生ストリーム
メディアデータ４０１
1 0 0 1 1 0 1 0

【書類名】要約書

【要約】

【課題】　ストリームメディアデータに対して高速な符号化と復号化を施し、スクランブル放送を符号化及び復号化のための専用ハードウェアなどを特に必要とせず簡単に行なうことを可能にする。

【解決手段】　配信側がストリームメディアデータを暗号鍵によって符号化して通信回線を介して配信し、受信側が配信されたストリームメディアデータを暗号鍵によって復号化するストリームメディアデータのスクランブル放送システムは、前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置３０を備え、前記配信側は、所定の時間的間隔で、鍵ビットパターン生成装置から生成される異なる鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行い、受信側は、配信側と同じ鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行う。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－３３５４０１
受付番号	５０２０１７４６５３３
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１４年１１月２０日

＜認定情報・付加情報＞

【提出日】　平成14年11月19日

次頁無

特願２００２－３３５４０１

出　願　人　履　歴　情　報

識別番号　　［０００００４２３７］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社

特願２００２－３３５４０１

出　願　人　履　歴　情　報

識別番号　　［０００２３２２５４］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都港区三田１丁目４番２８号
氏　名　　日本電気通信システム株式会社